CLAIMS

1. An access control protocol between an electronic key (EK_{kj}) and an electronic lock (B_i) performing access control, in which protocol, following presentation of said electronic key (EK_{kj}) to said electronic lock (B_i), a random variable message (a_{ij}) prompting authentication of the electronic key (EK_{kj}) is transmitted from said electronic lock to said electronic key, characterised in that, on receiving said random variable message (a_{ij}) prompting authentication, the protocol consists of at least, in succession:

- calculating and transmitting from said electronic key (EK_{kj}) to said electronic lock (B_i) a digital signature value of said random variable message prompting authentication based on a private signature key (K'_s) and specific authentication data), said specific authentication data transmitted by said electronic key (EK_{kj}) to said electronic lock (B_i) consisting of at least one public key (K'_p) certificate associated with said private signature key (K'_s), said public key certificate consisting of a digital signature value of at least one validity time period (PH_j) relating to a right of access and of said public key (K'_p), said signature value being calculated from another private signature key (K_s) associated with another public key (K_p), and, after reception by said electronic lock of said signature value (C_i) and said specific authentication data (Da_j):

- verification (1003) $v_{KPK'_P}((Ci,Daj))$by said electronic lock (B_i) of the authenticity of said signature value (C_i) as a function of said specific authentication data (Da_j) and, in response to a positive or negative result of said verification:

- acceptance or respectively refusal of said access.

2. A protocol according to claim 1, characterised in that said step of verification of said signature value

by said electronic lock includes, in succession:

- verification (1003a) by said electronic lock (B_i) of the authenticity of said specific authentication data based on comparison with reference data and, in the event of a positive result of said comparison:

- verification (1003b) by said electronic lock (B_i) of said signature value (C_i) as a function of said specific authentication data (Da_j).

3. A protocol according to claims 1 and 2, characterised in that said step of verification by said electronic lock of the authenticity of said specific authentication data (Da_j) consists of checking said validity time period (PH_j) associated with said public key (K'_P).

4. A protocol according to claim 2, characterised in that validity time period (PH_j) includes a plurality of non-contiguous time intervals.

5. A protocol according to claim 2 or claim 3, characterised in that each validity time period (PH_j) consists of at least one time interval having two limits each expressed as a date in terms of day, month, year and a time in terms of hour, minute, second.

6. A protocol according to any preceding claim, characterised in that said random variable message (a_{ij}) prompting authentication is a function of an identification value (C_i) of said electronic lock (B_i) and a continuously increasing variable value (CO).

7. A protocol according to any of claims 1 to 6, characterised in that, after reception of said random variable message (a_{ij}) prompting authentication by said electronic key (EK_{kj}) but before the step of calculation and transmission of a signature value (C_i) by said electronic key, said electronic key (EK_{kj}) having an internal clock, said protocol further consists of an auxiliary verification step (1007) for authorising

calculation of the signature of said random variable message prompting authentication, said auxiliary verification step (1007) consisting of:

- using the other public key (K_p) associated with said other private signature key (K_s) to verify (1007a) said public key (K'_p) certificate and said validity time period (PH_j) associated with said public key against said internal clock, to verify the validity of said public key),

- verifying (1007b) the association of said private signature key (K'_s) and said public key (K'_p), whose validity has been verified in the preceding step, and, on the basis of positive and negative result criteria (1007c) for the preceding two verification steps:

- continuing (1007e) or respectively interrupting (1007d) said access control protocol.

8. A protocol according to any of claims 2 to 7, characterised in that it further comprises a plurality of tests limiting all attack outside said validity time period, which tests are performed during said step of verification by said electronic lock (B_i) of the authenticity of said signature value (C_i), after said step (1003a) of verification by said electronic lock (B_i) of the authenticity of the specific authentication data (Da_j) consisting of checking said validity time period associated with said public key (K'_p) but before said step (1003b) of verification by said electronic lock (B_i) of the authenticity of said signature value, said protocol further comprising a plurality of tests ($1003a_1$) limiting any attack outside said validity time period (PH_j).

9. A protocol according to any of claims 1 to 8, characterised in that it comprises, before said step of calculation and transmission from said electronic key (EK_{kj}) to said electronic lock (B_i) of a signature value (C_i) of said random variable message (a_{ij}) prompting

authentication and specific authentication data (DA_j), said electronic key including a real-time clock:

- a step ($1007c_1$) of testing if a time variable delivered by said real-time clock is inside said validity time period (PH_j) and, in the event of a negative result of said test:

- a step ($1007c_3$) of invalidation of said electronic key interrupting said access control and leading to refusal of said access by said electronic lock.

10. An electronic key comprising cryptographic calculation means (C_{ak}) and message or data transmission means (T_k) for implementing a protocol according to any of claims 1 to 9 for controlling access to an electronic lock (B_i) by said electronic key (EK_{kj}), characterised in that, in addition to a central processor unit (CPU), said cryptographic calculation means (C_{ak}) include at least:

- a protected access memory area (1) for storing at least one private signature key (K'_s) and specific authentication data (Da_j), said specific authentication data (Da_j) consisting of at least one public key (K'_p) certiificate consisting of a digital signature value of at least one validity time period (PH_j) relating to a right of access and said public key (K'_p), and

- a read-only memory (4) used to call programs for calculating the digital signature value of a random variable message (a_{ij}) delivered by said electronic lock (B_i) using said private signature key (K'_s).

11. An electronic lock comprising cryptographic calculation means (C_{ai}) and message or data transmission means (T_i) for implementing a protocol according to any of claims 1 to 9 for controlling access to said electronic lock by an electronic key (EK_{kj}), characterised in that, in addition to a central processor unit (CPU), said calculation means (C_{ai}) include at least:

- a protected access memory area (5) for storing at

least one public signature verification key (K_p), and

- a read-only memory (6) used to call signature verification programs based on said at least one public key.